REMARKS/ARGUMENTS

I. Introduction:

Claims 1, 10, 15, 27, 32, 33, and 35 have been amended, claims 37-41 are added, and claims 9, 12, 13, 16, and 31 are canceled herein. With entry of this amendment, claims 1, 3-4, 6-8, 10, 11, 14, 15, 17-21, 23-30, and 32-41 will be pending.

Applicant respectfully requests reconsideration of the rejections set forth in the Office Action dated May 25, 2005 and consideration of new claims 37-41.

II. Claim Rejections – 35 U.S.C. 112:

In rejecting claims 32-34 under 35 U.S.C. 112, the Examiner states that "The specification does not make clear to one skilled in the art how the flow analyzer is able to identify if a rate of traffic exceeds a sampling capability of the aggregate filter." As noted in the specification at page 19, lines 8-15, for example, the flow analyzer may be configured to recognize that the total rate of traffic matching an aggregate value may far exceed its ability to sample by examining the statistics for the entry. In one example, the flow analyzer may identify that the total port traffic into a web server is too much for a filter assigned to that aggregate flow to handle. Applicant therefore submits that the limitation of claim 32 is described in the specification as to enable one skilled in the art to make and use the invention.

Claims 32 and 33 have been amended to replace "the aggregate filter" with "the filter".

Claim 35 has been amended to replace the term "flow cache" with flow cache entry", as requested by the Examiner.

III. Claim Rejections – 35 U.S.C. 101:

Claim 15 has been amended to specify that the computer-readable storage medium is not a data signal embodied in a carrier wave.

IV. Claim Rejections - 35 U.S.C. 103:

Claims 1, 3-4, 6-7, 9-13, 15-18, 20-21, 23-25, 27-30, and 35-36 stand rejected under 35 U.S.C. 103(a) as being unpatentable over WO 97/24841 (Cheriton et al.) in view of "Cisco Flow Logs and Intrusion Detection at the Ohio State University", (Romig et al.) and "Operating Firewalls Outside the LAN Perimeter", (Smith et al.).

Cheriton et al. disclose datagram transmission over virtual circuits. The invention of Cheriton et al. is directed to providing support for a wide range of network transmission speeds and a wide variety of source traffic behavior, while maintaining compatibility with existing network protocols and applications. The system processes network datagram packets in network devices as separate flows, based on the source and destination address pair contained in the datagram packet. This allows the network to control and manage each flow of datagrams in a segregated manner. Processing steps that can be specified for each flow include traffic management, flow control, packet forwarding, access control, and other network management functions.

As noted by the Examiner, the Cheriton et al. PCT application does not show or suggest creating an aggregate network flow summary for each network flow, analyzing at least one of the aggregate network flow summaries to detect characteristics of potentially harmful network flows, or generating a filter.

The Examiner cites Romig et al. as teaching that aggregating subsequent traffic in flow logs is beneficial. Romig et al. describe flow logs which capture a record of flows as they are removed from a flow cache. Romig et al. created a suite of tools to record and analyze flow logs. The flow logs may be used, for example, after an intrusion is reported to reach the captured flow logs and determine when the initial

attack occurred and what network traffic ensued from the victim host after the intrusion. The intrusion detection tools used by Romig et al. read through a set of previously captured flow logs (e.g., for a 24-hour period) and report on host and port scans. Other tools are used to investigate the intrusion more thoroughly (e.g., using flow-search and flow-print to extract specific records). The system is used to analyze data after an attack and does not provide for analysis as the attack is occurring. There is no filter generated to limit data coming into a network.

The Smith et al. reference teaches a firewall that works with intrusion detection software to automatically cause a set of firewalls to dynamically change security policy for individual attack activity. The gateway device acts as an autonomous system in policing activity of illegal hackers so that the blocking of unwanted inbound traffic is performed at the gateway network, rather than a network device within a corporate network. Thus, the data is being filtered before it gets to a network device that is operating as a firewall at a LAN operating within the corporate network.

Applicant respectfully submits that Cheriton et al., Romig et al., and Smith et al., either alone in combination, do not show or suggest creating an aggregate network flow summary for separate network flows, sending aggregate network flow summaries to a flow analyzer at a network device receiving the data, analyzing aggregate network flow summaries, and generating or refining a filter.

The tools disclosed by Romig et al. are used to analyze data after an attack and do not provide for analysis as the attack is occurring. Furthermore, Romig et al. do not teach sending an aggregate network flow summary to a flow analyzer located at the network device receiving the data.

Moreover, none of the references show or suggest selecting a new aggregate network flow summary to analyze and sending the selected aggregate network flow summary to a flow analyzer for analysis, wherein the new aggregate flow summary corresponds to network flow associated with the generated or refined filters, as set forth in amended claim 1.

Accordingly, claim 1 is submitted as patentable over Cheriton et al., Romig et al., and Smith et al.

Claims 3-4, 6-8, 10, 11, 14, 23-27, and 37-38, depending either directly or indirectly from claim 1, are submitted as patentable for the reasons discussed above with respect to claim 1.

Claim 27 is further submitted as patentable over the cited references, which do not show or suggest a class of packets to be analyzed selected based on statistics associated with a generated or refined filter. In rejecting claim 27, the Examiner refers to page 5 of Romig et al. This section of the paper simply discusses tools that are used to extract data from previously collected data.

Claims 15, 17, and 36 are directed to a computer program product for generating filters based on analyzed network flows and are submitted as patentable for at least the reasons discussed above with respect to claim 1.

Claim 18 is directed to a system for automatically generating filters based on data entering a network device and is submitted as patentable for the reasons discussed above with respect to claim 1. Claims 19-21 and 32-35, depending either directly or indirectly from claim 18, are submitted as patentable for the same reasons as claim 18.

Claims 8 and 19 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cheriton et al., Romig et al., and Smith et al. in further view of U.S. Patent No. 6,266,706 (Brodnik et al.). Brodnik et al. describe a fast routing lookup system. In rejecting these claims, the Examiner refers to col.2, line 64 - col. 3, line 3 of the Brodnik et al. patent. In this prior art section, Brodnik et al. note that IP router designs use special-purpose hardware to do IP processing. However, Brodnik et al. go on to describe how this can be an inflexible solution since any changes in the IP format or protocol could invalidate such designs and the flexibility of software makes it a more preferable solution. Brodnik et al. also note that using hardware to do routing lookups is an expensive solution. Brodnik et al. thus, teach away from using hardware to send each network flow to a corresponding flow cache. Applicant is not implying that Brodnik is

teaching away from using both software and hardware, as obviously both are required. (see, Response to Arguments in Office Action dated May 25, 2005). Instead Applicant notes that Brodnik teaches away from using special-purpose hardware to do IP processing and does not teach using hardware to send network flow to a corresponding flow cache and using software to analyze network flow. Accordingly, claims 8 and 19 are submitted as patentable.

The other references cited, including U.S. Patent Nos. 6,389,532 (Gupta et al.), 6,651,099 (Dietz et al.), and 6,667,985 (Drummond-Murray), do not remedy the deficiencies of the primary reference.

V. Conclusion:

For the foregoing reasons, Applicant believes that all of the pending claims are in condition for allowance and should be passed to issue. If the Examiner feels that a telephone conference would in any way expedite the prosecution of the application, please do not hesitate to call the undersigned at (408) 399-5608.

Respectfully submitted,

Cindy S. Kaplan
Reg. No. 40,043

P.O. Box 2448
Saratoga, CA 95070
Tel: 408-399-5608
Fax: 408-446-8691